TAB B Cloud Contracting Language

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-3: Metadata about all Army data assets must be registered in the Army Enterprise Data Service Catalog (EDSC) and comply with Dublin Core Metadata Element Sets and International Standards Organization Metadata Registries requirements.	The contractor shall ensure that all Army data assets are registered in the Army Enterprise Data Service Catalog (EDSC) and comply with Dublin Core Metadata Element Sets and International Standards Organization Metadata Registries requirements.	Required	Required	Required	N/A	Yes	No	No
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-5: Data must be managed across its lifecycle and captured in a data management plan.	N/A	Required	Required	Required	N/A	Yes	Yes	No
DFARS 239.7602-2(b), Required Storage of Data within the United States or Outlying Areas: All data will reside physically within the legal jurisdiction of the United States. If the location of the data is not physically maintained within the legal jurisdiction of the United States, written determination from the Contracting Officer to authorize use of another location is required IAW DFARS 239.7602-2(b).	The Contractor shall maintain all data within the legal jurisdiction of the United States IAW DFARS 239.7602-2(b).	Required	Required	Required	Required	Yes	Yes	Yes
(1) HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration,(15 November 2019) (2) Cost Report (Cost Summary Data Report 1921, 1921-5) (3) Contract Work Breakdown Structure (CWBS) Dictionary	The Contractor shall ensure that all cloud-related costs/price, which include but are not limited to: cost of modernization and migration of applications, Cloud Service Provider (CSP) costs, and cloud Operations and Maintenance (O&M) costs/prices are clearly identified and available for government reporting purposes.	Required	Required	Required	Required	Yes	No	No

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
DUSA Cloud Requirements Memo, 15Jan2021: The Army will modernize applications applying Cloud Native Design Principles, which will prioritize the use of Software as a Service (SaaS) and Platform as a Service (PaaS) design patterns and automation to reduce technical debt, management toil, and overhead of maintaining IT systems to increase mission value and mission investments.	The contractor shall modernize applications migrating to commercial cloud applying Cloud Native Design Principles and shall prioritize use of Software as a Service (SaaS) and Platform as a Service (PaaS) over Infrastructure as a Service (IaaS).	Required	N/A	N/A	N/A	Yes	No	No
Army CIO memo "SUBJECT: Update to Army Cloud Computing Requirements "	The contractor shall ensure that legacy systems undergoing modifications to adapt to a service-enabled architecture will include the design of anti-corruption layers to support the transitional period.	Required except pre-bundled COTS products	N/A	N/A	N/A	Yes	No	No
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020) - Principle DSR-6: All new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification).	The contractor shall ensure that all new and existing applications, systems, or services deemed non-legacy shall expose their data and functionality through service interfaces (for example, OpenAPI specification).	Required	Required	Required	N/A	Yes	No	No
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020) - Principle DSR-7: All service interfaces, without exception, must be designed to be consumable from external sources and must plan and design to be able to expose the interface to developers.	The contractor shall ensure that all data is exposable and consumable through external service data interfaces that are versioned, published, secured, and discoverable to other capability developers and consumers. The contractor shall utilize the modular open systems approach (MOSA) as defined by the Government. (https://www.dsp.dla.mil/Programs/MOSA/)	Required	Required	Required	N/A	Yes	No	No

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020) - Principle DSR-4: All Army data sources must be developed with built-in data exchange capabilities. Data mapping must also be implemented to increase efficiency and ease of use of data assets as they are being translated or transformed. At a minimum, programs and initiatives are required to comply with Global Force Management Data Initiative; International Standards for dates; Geopolitical Entities, Names and Codes, Common (GENC); Joint Consultation, Command and Control Exchange Data Model; or Resource Description Framework standards and schemas.	The contractor shall ensure that All Army data sources are developed with built-in data exchange capabilities. Data mapping shall also be implemented to increase efficiency and ease of use of data assets as they are being translated or transformed. At a minimum, programs and initiatives are required to comply with Global Force Management Data Initiative; International Standards for dates; Geopolitical Entities, Names and Codes, Common (GENC); Joint Consultation, Command and Control Exchange Data Model; or Resource Description Framework standards and schemas.	Optional	Required	Optional	N/A	Yes	No	No
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020) - Principle DSR-9: There will be no other form of Inter-Process communication allowed: no direct linking, no direct reads of another data store, no shared-memory model, and no back-doors whatsoever. The only Inter-Process communication allowed is intra-system data exchanges or service interface calls over the network. All other requests or methods require CIO approval.	The contractor shall ensure that there will be no other form of Inter-Process communication allowed: no direct linking, no direct reads of another data store, no shared-memory model, and no back-doors whatsoever. The only Inter-Process communication allowed is intra-system data exchanges or service interface calls over the network.	Optional	Required	Optional	N/A	Yes	No	No
Army CIO memo "SUBJECT: Update to Army Cloud Computing Requirements "	The contractor shall use modern software development methodologies (e.g., Agile, DevSecOps) to support rapid delivery of standardized, reliable, integrated and secure mission capabilities.	Optional	Required	Optional	N/A	Yes	No	No
Army Cloud Plan, 2022: All new software acquisitions should use microservices architecture and automation where technically and economically feasible.	The contractor shall use microservices architecture and automation where technically and economically feasible.	Optional	Required	Optional	N/A	Yes	No	No

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
Army Cloud Plan, 2022: In alignment with the DoD Software Modernization Strategy published in February 2022, CReATE will expand to enable continuous risk management framework (cRMF) activities to accelerate authorized deployments of software. The standardization of CReATE's DevSecOps tools and cARMY's continued development of common shared services streamlines the accreditation process, reduces technical debt, and increases the Army's security posture.	The contractor shall maximize the use of the Army's Coding Repository and Transformation Environment (CReATE) tools and services where technically and economically feasible.	Required	Required	Required	N/A	Yes	No	No
Army Cloud Plan, 2022: In order to create interoperable, accessible and visible services, all interface information will be published in the Army Enterprise Data Services Catalog (EDSC).	The contractor shall comply with publishing all application programming interface (API) information/metadata within the Enterprise Data Services Catalog (EDSC)	Required	Required	Required	N/A	Yes	Yes	No
Army Cloud Plan, 2022: The Army will build to the highest abstraction of cloud services, where possible, to include SaaS, PaaS, Database Management as a Service, and so forth, in order to accelerate testing, accreditation and fielding to the Army. Use of IaaS will be by exception and at the approval of the Enterprise Cloud Management Agency (ECMA).	The contractor shall build to the highest abstraction of cloud services in order to meet functional, technical, performance and cost goals. These services include commercial SaaS, PaaS, Database Management as a Service, and so forth, in order to accelerate testing, accreditation and fielding to the Army.	N/A	Required	N/A	N/A	Yes	No	No

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
(1) Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-1; (2) Impact-level Guidance for Data Migrating to Army-approved Cloud Environments (1 May 2020); (3) Authorization Guidance for IT Capabilities Migrating to Army-approved Cloud Environments (1 May 2020); Reference DoD Instruction 8580.1, Information Assurance (IA) in the Defense Acquisition System (9 July 2004), each DoD information system is required to have an Information System Security Manager (ISSM) and must implement DoD Risk Management Framework (RMF) governed by DoD Instruction 8510.01, for DoD Information Technology (IT). All cloud instances will inherit RMF controls to the greatest extent allowable by the Authorizing Official.	The contractor shall comply with implementation of the DoD Risk Management Framework (RMF) as governed by DoD Instruction 8510.01, for DoD Information Technology (IT).	Required	Required	Required	Required	Yes	Yes	No
Deputy Under Secretary of the Army, Army Enterprise Cloud Services and Modernization, 15 January 2021: All Army cloud instances will use Army Future Command (AFC)'s Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (C5ISR) as their Cybersecurity Service Provider (CSSP). Exceptions can only be granted by the Army Cyber Command (ARCYBER) or the Chief Information Officer (CIO).	The contractor shall work with Army Future Command (AFC)'s Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center (C5ISR) or other ARCYBER-designated Cyber Security Service Provider (CSSP) to establish CSSP services (as required by DoDI 8530 and as described by the DISA Cloud Computing Security Requirements Guide) for Army applications hosted in commercial cloud.	Required	Required	Required	N/A	Yes	Yes	Yes
DoD Cloud Computing Security Requirements Guide (DoD CC SRG) Version 1 Revision 4, Section 6.5.1, IAW DFARS 239.7604: The Army must adhere to the DoD Cloud Computing Security Requirements Guide version 1 release 4 (or superseding versions or releases). IAW DFARS 239.7604	The contractor shall adhere to the DoD Cloud Computing Security Requirements Guide version 1 release 4 (or superseding versions or releases). In particular, the contractor shall provide security incident response plans, and shall update the plans on an annual basis, or when a significant change occurs to the technical or operational environment.	Required	Required	Required	Required	Yes	Yes	Yes

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
DoD Cloud Computing Security Requirements Guide (DoD CC SRG) Version 1 Revision 4, Section 4: Contracts shall only be awarded to a cloud service provider that DISA granted a DoD Provisional Authorization (PA), at the level appropriate to the requirement, to deliver the relevant cloud computing model IAW with the DoD CC SRG.	The Contractor shall ensure that the cloud environment fully complies or exceeds the security requirements for impact level _(insert level here)__in the DoD Cloud Computing Security Requirements Guide (SRG) version 1 release 4 (or superseding versions or releases). The Contractor shall make the environment accessible for a DoD security team to evaluate the environment prior to the placement of any DoD data in the environment and allow for periodic security reviews of the environment during the performance of this contract.	Required	Required	Required	Required	Yes	Yes	Yes
Committee on National Security Systems Policy (CNNSP) 15; Army Regulation 25-2: Army Cybersecurity (4 May 2019): Data must be encrypted at rest and in-transit	The contractor shall ensure that all data-at-rest and data in-transit is encrypted utilizing NSA-approved encryption.	Required	Required	Required	Required	Yes	Yes	Yes
DoD CC SRG Version 1 Revision 4: Section 6: Cyberspace Defense and Incident Response	The Contractor shall provide U.S. Army Cyber Command relevant access for Army Defensive Cyber Operations (DCO) elements to operate with appropriate access permissions to enable DCO maneuver and response within a timely manner based on severity of incident	Required	Required	Required	Required	Yes	No	No
DoD CC SRG Version 1 Revision 4: Section 6: Cyberspace Defense and Incident Response	The Contractor shall provide U.S. Army Cyber Command read access to any logging or Security Information and Event Management (SIEM) data and will configure manual or automated export of logging or SIEM data to Army or other government sources on request	Required	Required	Required	Required	Yes	No	No
DoD CC SRG Version 1 Revision 4: Section 6: Cyberspace Defense and Incident Response	For IaaS environments, the contractor shall provide U.S. Army Cyber Command appropriately configured cloud infrastructure for Army Defensive Cyber Operations (DCO) elements to operate from when directed by the United States Government.	Required	Required	Required	Required	Yes	No	No
DoD CC SRG Version 1 Revision 4: Section 6: Cyberspace Defense and Incident Response	Upon request by the USG, the contractor shall provide ARCYBER with access to additional information or equipment that is necessary to conduct a forensic analysis.	Required	Required	Required	Required	Yes	No	No

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
DoD CC SRG Version 1 Revision 4: Section 6: Cyberspace Defense and Incident Response	During identified/suspected potential malicious cyber activity (MCA) or cyber security incident, the contractor shall provide U.S. Army Cyber (ARCYBER) all information related to the event, upon request by ARCYBER [DoD Event Category 5 and above within 3 hours or less, DoD Event Category 2-4 within 72 Hours.]. Information provided would include but not be limited to: Owning organization/POC, Tenant ID/subscription ID, Resource Group/VPC information, Hostname, IP space, etc. (1) The contractor shall provide ARCYBER all Government data and Government-related data in the format specified by ARCYBER. (2) The Vendor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to ARCYBER in accordance with contract closeout procedures. (3) The contractor shall provide the ARCYBER, or its authorized representatives, access to all Government data and Government-related data, access to contractor personnel involved in performance of the contract, and physical access to any Contractor facility with Government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.	Required	Required	Required	Required	Yes	No	No
HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration, 3.E.7.D. All Army systems/applications developed in, migrated to and hosted in the commercial cloud will use cArmy Enterprise common services and data services to achieve the Army Data Plan objectives for cloud consolidation. The Army will not duplicate common services or data services that are accredited in cArmy, to include the components of the DoD Secure Cloud Computing Architecture (SCCA). If a service is required that is not yet available in cArmy, the Application/System Owner must work with the Enterprise Cloud Management Agency (ECMA) before any development of that service occurs (or any dollars are obligated towards the development). A list of the currently available services is found at army.mil/ecma. Exceptions to this policy can only be granted by the ECMA.	The contractor shall use cArmy Enterprise common services, data services, and all DoD Secure Cloud Computing Architecture (SCCA) components when developing, migrating to and hosting Army systems/applications in the commercial cloud.	Required	Required	Required only for Application Operations and Continual Enhancement	N/A	Yes	Yes	No

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration, 3.E.7.D. Existing cloud common services will be consolidated into cArmy as is reasonable over time, per EXORD 009-20. As existing common service contract options expire, mission owners should work with the Enterprise Cloud Management Agency (ECMA) to onboard their applications into cArmy and reduce the duplicity of services across the Army.	N/A	N/A	N/A	Required only for follow on contracts related to common services and management	N/A	Yes	No	No
Deputy Under Secretary of the Army, Army Enterprise Cloud Services and Modernization, 15 January 2021: Procurement of all DoD Information Impact Level (IL) 6 and below Cloud Service Provider (CSP) Offerings will use the Army's Enterprise CSP Reseller contract. Exceptions to this policy include programs funded by Military Intelligence Program (MIP)/National Intelligence Program (NIP) monies. Other exceptions can only be granted by the ECMA. As contract options expire, existing CSP service contracts will also be migrated to the Army's Enterprise CSP reseller contract.	The Government will provide all Cloud Service Offering (CSO) requirements, at the required DoD Information Impact Level (IL) including IL2, IL4, IL5, and/or IL6 that are within scope of the Army Enterprise Cloud Contract Vehicle, as Government Furnished Equipment (GFE). The Government will furnish the tenant account administrative credentials or the appropriate role / Identity and Access Management (IAM) as Government Furnished Information (GFI) to the contractor to manage in accordance with Government policies. The contractor will not have access to Root administrator credentials.	Required	Required	Required	Required	Yes	Yes	No
HQDA EXORD 009-20: Army Data Plan Implementation in Support of Cloud Migration,(15 November 2019): All commercial cloud usage must be reported into the Army Portfolio Management System (APMS) per data EXORD 009-20	N/A	Required	Required	Required	Required	Yes	Yes	Yes

		Cloud Activities / CLIN Name				Contract Actions		
Policy Reference(s) (when applicable)	**Mandatory Performance Work Statement (PWS) Language**	**1a) Migrating to the Cloud**	**1b) New Software (SW) Development in the Cloud**	**2) Application Operations and Continual Enhancement in the Cloud and/or follow-on contracts related to common services and management**	**3) Cloud Hosting**	**New Contracts/Task Orders**	**Orders Against Existing Contracts/Task Orders**	**Existing Contracts/Task Orders**
Mandatory Implementation of Army Data Standards Services Requirements Memo (10 April 2020), Principle DSR-8: All custom software or customized COTS software written by the Army or developed with Army funding will be centrally controlled and made available to all DoD, IC and inter-agency partners within the approved Army source code repositories on the Unclassified, Secret, and Top Secret networks in accordance with Army Directive 2018-26 (Enabling Modernization Through the Management of Intellectual Property).	The contractor shall utilize government approved centralized source code repositories to store all government funded software development or customization of COTS products.	Required	Required	Required	N/A	Yes	No	No

Parent topic: APPENDIX HH SUBPART - CLINS